

FREQUENTLY ASKED QUESTIONS (FAQS)
**Minnesota Statutes, section 62J.536 and related rules for the
standard, electronic exchange of health care administrative
transactions**

The following FAQs are provided for information and clarification. They will be revised and updated as needed. Additional information regarding Minnesota Statutes § 62J.536 and related rules is available at www.health.state.mn.us/asa.

Last Revised: 09-15-09

Categories of FAQs

I. MORE ON THE LAW AND RULES (WHAT THE LAW DOES, WHY IT WAS PASSED, WHO IT APPLIES TO, ETC.)

II. ADDITIONAL GENERAL INFORMATION (HOW TO OBTAIN COPIES OF THE RULES, BACKGROUND ON THE AUC, DESCRIPTIONS OF TRANSACTIONS, ETC.)

III. COMPLIANCE AND ENFORCEMENT BY THE MINNESOTA DEPARTMENT OF HEALTH (MDH) (BEFORE REVIEWING THESE FAQs, PLEASE SEE ALSO CATEGORY I ABOVE)

IV. FEDERAL HIPAA REGULATIONS (HIPAA TRANSACTIONS AND CODE SETS RULES; HIPAA PRIVACY AND SECURITY RULES)

V. IMPLEMENTATION, BECOMING COMPLIANT WITH THE LAW AND RULES

VI. QUESTIONS SPECIFIC TO EACH OF THE COVERED TRANSACTIONS (ELIGIBILITY INQUIRY AND RESPONSE; CLAIMS; PAYMENT AND REMITTANCE ADVICE)

VII. OTHER/MISC.

FAQs with Answers

I. MORE ON THE LAW AND RULES (WHAT THE LAW DOES, WHY IT WAS PASSED, WHO IT APPLIES TO, ETC.)

1) What does the law (Minnesota Statutes, section 62J.536) do?

Answer: The law simplifies, standardizes and automates three types of common health care business transactions:

1. Checking a patient's eligibility and reporting back eligibility status;
2. Submitting and adjudicating claims; and
3. Producing and receiving a remittance advice (RA).

These transactions must be transmitted electronically between providers and payers, using a single, uniform, standard data content and format, beginning on three different dates in 2009.

The law also requires the Minnesota Department of Health (MDH) to develop rules for the standard data content and format of the transactions. MDH must consult on the rules with a large, voluntary stakeholder group, the Minnesota Administrative Uniformity Committee (AUC). The rules are to be based on federal HIPAA transactions and code sets regulations (see Q&A below) and Medicare, although exceptions from Medicare standards are permitted in developing the rules. The rules were adopted in 2008, at least one year before having the effect of law in 2009. MDH administers the law and the related rules, including compliance and enforcement.

2) When does the law and the related rules take effect?

Answer: As required by the law, rules for the standard, electronic exchange of the health care transactions below were adopted in 2008 and have the force of law as follows:

Health Care Administrative Transaction	Date That Rules Have the Force of Law
Eligibility Inquiry and Response (ANSI X12 270/271)	January 15, 2009
Claims (ANSI X12 837 Professional, Institutional and Dental as well as the NCPDP 5.1 Pharmacy Claim and Reversal, Submission and Response)	July 15, 2009
Health Care Claims Payment Remittance Advice (ANSI X12 835).	December 15, 2009

3) Why was this law enacted?

Answer: Paper and nonstandard electronic health care transactions are expensive and inefficient for providers, payers, consumers, and government alike. This law is intended

to improve efficiency, and applies to all providers and payers to get the most benefit from electronic, standard exchanges. Electronic data interchange can also speed up reimbursement time and enhance the accuracy of a claim before it is submitted for adjudication.

4) Who does the law and rules apply to? Who must follow the law? How do I know if Minnesota’s requirements for standard, electronic health care business transactions apply to me/my organization?

Answer: The law applies to all health care providers who provide services for a fee in Minnesota, and all group purchasers (insurance companies, health plans, and other payers) licensed or doing business in Minnesota.

More specifically, Minnesota Statutes, section 62J.536 and related rules apply to covered transactions between:

- All health care providers providing services for a fee in Minnesota and who are otherwise eligible for reimbursement under the Minnesota Medical Assistance (Medicaid) program. (“Eligible for reimbursement under the Medical Assistance program” means that the provider’s services would be reimbursed by the Minnesota Medical Assistance program if the services were provided to Medical Assistance enrollees and the provider sought reimbursement”.);

and

- “Group purchasers” (payers) licensed or doing business in Minnesota. Group purchaser is further defined in Minnesota Statutes, section 62J.03, as a “a person or organization that purchases health care services on behalf of an identified group of persons, regardless of whether the cost of coverage or services is paid for by the purchaser or by the persons receiving coverage or services”. The definition of “group purchaser” includes not only group health insurance, but also property-casualty insurance carriers, workers’ compensation carriers, auto carriers, TPAs, and other payers. The definition applies to individual as well as group coverage, and for both “open” and “closed” books of business.

This means that:

1. If your organization is licensed or doing business in Minnesota as an insurer, TPA, or other health care payer
And
2. if your organization (or someone on your behalf) is paying, or could potentially have to pay for medical, dental, or pharmacy claims
3. from a doctor, hospital, or other health care provider who is billing you for services they provided in Minnesota for a fee
Then
4. the law (Minnesota Statutes, section 62J.536) applies to you.

4a) What is the definition of health care provider referenced in the statute?

Answer: As noted above, under Minnesota law (Minnesota Statutes, section 62J.03 and Minnesota Statutes, section 62J.536), a health care provider is defined as “a person or organization ... that provides health care or medical care

services within Minnesota for a fee and is eligible for reimbursement under the medical assistance program”.

The definition of health care provider includes:

- Advanced Practice Registered Nurses
- [Alternative Care \(AC\)](#)
- Ambulatory Surgical Centers
- Audiologists
- [CAC](#)
- [CADI](#)
- Certified Nurse Midwives
- Certified Registered Nurse Anesthetists
- Chemical Dependency Treatment
- Child and Teen Checkup (C&TC)Clinics
- Chiropractors
- Clinical Nurse Specialists
- Community Health Clinics
- Community Mental Health Centers
- County Case Managers
- County Contracted Mental Health Rehabilitative Services
- County Human Services Agencies
- Day Training and Habilitation (DT & H) Centers
- Day Treatment Programs
- [DD waiver](#)
- Dental Labs
- Dentists/Dental Groups
- DME
- [Elderly Waiver](#)
- Family Planning Agencies
- Federally Qualified Health Centers
- Head Start Agencies
- Hearing Aid Dispensers
- Home Health Agencies
- Hospices
- Hospitals
- Independent Diagnostic Testing Facilities
- Independent Laboratories
- Indian Health Services
- Institutions for Mental Disease
- Intermediate Care Facilities for the Mentally Retarded (ICF/MRs)
- Interpreter services
- Licensed Independent Clinical Social Workers
- Licensed Marriage and Family Therapists
- Licensed Nutritionists
- Licensed Psychological Practitioners
- Licensed Registered Dieticians
- Managed Care Organizations
- Medical Suppliers/Durable Medical Equipment (DME)
- Medical Transportation
- Mental Health Targeted Case Management
- Nurse Practitioners

- Nursing Homes
- Occupational Therapists
- Optical Companies
- Optometrists
- Personal Care Provider Organizations
- Pharmacies
- Physical Therapists
- Physician Assistants
- Physicians/Clinics
- Podiatrists
- Private Duty Nurses/Private Duty Nursing Agencies
- Psychiatrists
- Psychologists
- Public Health Clinics
- Public Health Nursing Agencies
- Regional Treatment Centers
- Registered Nurses (RN)/Licensed Practical Nurses (LPN)
- Rehabilitation Agencies
- Renal Dialysis
- Rural Health Clinics
- School Districts (IEP)
- Speech Language Pathologists
- [TBI](#)
- Translator services
- Transportation
- Waivered (Home & Community-Based) Services
- Women, Infants, & Children (WIC) Programs
- X-Ray

For the purposes of Minnesota Statutes, section 62J.536, the definition of “health care provider” does not include acupuncturists, massage therapists, naturopaths, or other service providers who are ineligible for reimbursement under the Minnesota Medical Assistance (Medicaid) Program.

NOTE: Providers that are not eligible to obtain an NPI from CMS are defined as “atypical” providers in the [Minnesota Uniform Companion Guides for Implementation of the Health Care Claim](#) (versions Professional, Institutional and Dental). The Administrative Simplification rules do apply to these atypical providers. If the provider is not eligible to obtain an NPI (and is therefore considered “atypical”) then the primary provider identifier on the claim is the TIN and a secondary identifier is allowable. The qualifier on the claim for the secondary identifier would be “G2.” The identifier for this qualifier would be a payer assigned identifier.

4b) What is the definition of group purchaser? Does it apply to workers’ compensation, property and casualty, and auto insurance carriers?

Answer: As noted above, Minnesota Statutes, section 62J.03 defines “group purchaser” “*a person or organization that purchases health care services on behalf of an identified group of persons, regardless of whether the cost of*

coverage or services is paid for by the purchaser or by the persons receiving coverage or services". The definition of "group purchaser" includes insurance carriers and third party administrators licensed or doing business in Minnesota. The definition includes not only group health insurance, but also:

- property-casualty insurance carriers;
- workers' compensation carriers;
- auto carriers;
- Third Party Administrators (TPAs);
- the Minnesota Department of Human Services, which administers Medical Assistance, MinnesotaCare, and other programs; and
- other payers.

The definition of group purchaser applies to individual as well as group coverage, and for both "open" and "closed" books of business. The definition applies regardless of whether the entity is actively marketing or servicing policies in Minnesota or not.

A preliminary, informational list of HMOs, insurance carriers, and TPAs that are licensed in Minnesota and that have been identified as meeting the definition of group purchaser is listed at www.health.state.mn.us/asa. (Note: This list is intended only as an informational resource. It is maintained to be as accurate as possible given information available but is subject to change. It is NOT a legal determination by the State of Minnesota or any other organization of all possible payers covered by Minnesota Statutes, section 62J.536.)

4c) Do the requirements of Minnesota Statutes, section 62J.536 apply to Medicaid subrogation or other payer to payer exchanges?

Answer: The requirements for standard, electronic exchanges of health care administrative transactions apply only to HIPAA-covered transactions. HIPAA does not include Medicaid subrogation, and Minnesota's requirements do not apply to Medicaid subrogation or other payer to payer exchanges.

4d) Do the requirements apply to secondary and tertiary payers? Do the law and rules apply to Coordination of Benefits (COB?)

Answer: Yes, Minnesota's rules apply to secondary and tertiary payers other than claims which are electronically crossed over from Medicare to another Minnesota payer. Instructions on sending prior payer adjudication information on a subsequent claim submission are found in sections 4.2.3.5.1 and 4.2.3.5.2 of the Minnesota Uniform Companion Guides (rules) for the 837 Institutional and 837 Professional transactions. (The rules are available at no charge at: <http://www.health.state.mn.us/asa/rules.html>.)

Additional information on COB exchanges can be found in the listings of "best practices" at the Minnesota Administrative Uniformity Committee (AUC) website at:

Professional services - <http://www.health.state.mn.us/auc/profguide.htm>;
Institutional services - <http://www.health.state.mn.us/auc/instguide.htm>;
Dental services - <http://www.health.state.mn.us/auc/dentguide.htm>.

(For more information on the “Best practices” concept generally, please see the answer to FAQ Section II, number 3.)

4e) Do the law and rules apply to clearinghouses, billing services, software vendors, and other vendors or service providers?

Answer: The law and rules apply to transactions between health care providers and group purchasers (payers). However, in order for providers and payers to be compliant, they will need their vendors and service providers to also be compliant on their behalf.

4f) What if we are an insurance carrier in Minnesota, but we no longer write policies here? Do the law and rules still apply?

Answer: Yes, the law and rules still apply to “closed” books of business as well as open books of business. Even if you no longer write (or never wrote) policies in Minnesota, if you are licensed or doing in business in Minnesota and if you could be responsible for medical claims incurred by your insured(s) for treatment from a health care provider providing their services for a fee in Minnesota, the law and rules apply.

4g) My organization pays the insurance policy holder directly for care provided. We never pay a health care provider. Does the law apply to us?

Answer: While we encourage the use of standard, electronic health care transactions as widely as possible, Minnesota’s law and rules apply to covered exchanges between health care providers and group purchasers. Claims submitted directly by the insured/patient to a payer are not part of the requirements.

5) Are there any exceptions to the law’s requirements?

Answer: Minnesota Statutes, section 62J.536 does NOT apply to:

- Transactions with Medicare or Medicare Advantage products; or
- Claims submitted by a patient/insured directly to the insurer/payer.

Please also note: The statute allows for only one other very limited, targeted exception, for only group purchasers not covered by federal HIPAA regulations, where the following criteria are met:

- (i) a transaction is incapable of exchanging data that are currently being exchanged on paper and is necessary to accomplish the purpose of the transaction; or
- (ii) another national electronic transaction standard would be more appropriate and effective to accomplish the purpose of the transaction.

The above criteria have been met, and an targeted, very limited exception from the rules has been granted, ONLY to payers not covered by federal HIPAA transactions and code sets requirements (i.e., property and casualty, auto, and workers’ compensation carriers) and ONLY from the requirement to electronically exchange eligibility inquiries and

responses. However these carriers must still comply with the requirements for the standard, electronic exchange of claims and payment remittance advices.

5a) Can small providers such as those without computers or with few transactions receive an exception or be allowed to delay implementation? Can small payers not covered by federal HIPAA transactions and code sets regulations receive an exemption?

Answer: No. The only exceptions to the requirements in Minnesota Statutes, section 62J.536 are those noted in answer 5 above. Minnesota Statutes, section 62J.536 and related rules apply to all health care providers, as well as all group purchasers (payers) as described above.

The benefits of standardization are greatly reduced or lost when there are exceptions or exemptions. Providers and payers have a number of options to comply with the law and rules that best meet their business needs, including a wide variety of arrangements, vendors, and service providers. In addition, while there may be start-up and transition costs to become compliant with the law and rules, the standard electronic transactions will also result in quicker payment, and more efficient transactions, less costly transactions over time.

II. ADDITIONAL GENERAL INFORMATION (HOW TO OBTAIN COPIES OF THE RULES, BACKGROUND ON THE AUC, DESCRIPTIONS OF TRANSACTIONS, ETC.)

1) Where can I find copies of the statute and rules? Do they cost anything?

Answer: Copies of the statute and the Minnesota Uniform Companion Guides (rules) are available at: <http://www.health.state.mn.us/asa>. There is no cost for accessing the Guides via the website.

2) What are “companion guides”? What is the relationship between the rules and “Minnesota Uniform Companion Guides”? Are the rules the same as the “Minnesota Uniform Companion Guides”?

Answer: To answer this question we first provide some background. In 2003, the US federal government implemented regulations under HIPAA for transactions and code sets requirements for the electronic exchange of health care administrative transactions. The regulations require that the transactions be exchanged according to “Implementation Guides” that specify the permitted data content and format for the transactions.

The HIPAA Implementation Guides (IGs) allow individual customization of the data content and format within overall limits. Users of the HIPAA IGs created additional “companion guides” to be used in conjunction with (as “companions” to) the HIPAA IGs, to describe their customization of the IGs. Over time, as payers have implemented their particular customizations of the HIPAA IG data content and format, the number of companion guides has proliferated. This growth of individual companion guides has offset some of the benefits of data standardization that were the basis of the HIPAA IGs.

Minnesota Statutes, section 62J.536 requires the Minnesota Department of Health (MDH) to consult with the Minnesota Administrative Uniformity Committee (AUC), on the development and adoption of single, uniform companion guides to the HIPAA implementation guide. Rather than allowing administrative transactions to be exchanged according to many different payer-specific companion guides, Minnesota requires that all providers and payers exchange the transactions according to a single, uniform companion guide. These “Minnesota Uniform Companion Guides” have been adopted into rule with the force of law. The Minnesota Uniform Companion Guides are the rules required under MN Statutes § 62J.536. These Companion Guides comply with the HIPAA Implementation Guides and are to be used as the single, uniform companion guides to the HIPAA IGs.

In summary, the Minnesota Uniform Companion Guides:

“...specif[y] the requirements to be used when preparing, submitting, receiving and processing electronic health care administrative data. The document supplements, but does not contradict, disagree, oppose, or otherwise modify the HIPAA Implementation Guide in a manner that will make its implementation by users to be out of compliance. Using this [Minnesota] Companion Guide does not mean that a claim will be paid. It does not imply payment policies of payers or the benefits that have been purchased by the employer or subscriber.”

3) What are the AUC’s “Best Practice” documents? What is the difference between the MN Uniform Companion Guides and the AUC Best Practices documents?

Answer: The Minnesota Uniform Companion Guides are rules for the standard data content and format of standard, electronic health care administrative transactions (see additional description in answer for question 2 immediately above). They are mandatory and have the force of law. The Guides (rules) are available at: <http://www.health.state.mn.us/asa/>.

The Minnesota Department of Health (MDH) is consulting on the rules with the Minnesota Administrative Uniformity Committee (AUC – see also the answer to question 4, following). Best Practices documents are consensus recommendations of the AUC to further standardize and harmonize health care administrative transactions. However, Best Practices documents are not mandatory and do not have the force of law. While adoption or adherence to the Best Practices is voluntary, it is strongly encouraged to further reduce health care administrative burdens and costs. The AUC Best Practices (as well as additional copies of the rules described above) can be found at the AUC website at:

<http://www.health.state.mn.us/auc/profguide.htm> (for professional services);

<http://www.health.state.mn.us/auc/instguide.htm> (for institutional services);

<http://www.health.state.mn.us/auc/dentguide.htm> (for dental services);

<http://www.health.state.mn.us/auc/pharmguide.htm> (for pharmacy services).

4) I am not familiar with the transactions covered by the law. What is an “eligibility inquiry and response”? What is a “health care claim”? What is a “health care claim payment and remittance advice”?

Answer: Minnesota has developed rules for the standard, electronic exchange of three types of health care administrative transactions, as described below:

- The **eligibility for a health plan transaction** is the transmission of either of the following:
 - (a) An inquiry from a health care provider to a group purchaser, or from one group purchaser to another group purchaser, to obtain any of the following information about a benefit plan for an enrollee:
 - (1) Eligibility to receive health care under the group purchaser.
 - (2) Coverage of health care under the group purchaser.
 - (3) Benefits associated with the group purchaser.
 - (b) A response from a group purchaser to a health care provider's (or another group purchaser's) inquiry described in paragraph (a) of this section.

- The **health care claims or equivalent encounter information transaction** is the transmission of either of the following:
 - (a) A request to obtain payment, and the necessary accompanying information from a health care provider to a group purchaser, for health care.
 - (b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care.

- The **health care payment and remittance advice transaction** is the transmission of the following from a group purchaser to a health care provider:
 - (1) Explanation of benefits.
 - (2) Remittance advice.

Please also note: The Minnesota Department of Health (MDH) encourages electronic payment (electronic funds transfer, EFT) as a further means of reducing health care administrative costs and burdens. However, MN Statutes § 62J.536 does not require electronic payment (EFT). Group purchasers and providers may be subject to other requirements or trading partner agreements which require the transmission of an electronic payment. It is recommended that each organization familiarize itself with its payment procedures as it may relate to the remittance advice implementation date.

5) What is the Minnesota Administrative Uniformity Committee (AUC?)

Answer: The Minnesota Department of Health (MDH) is statutorily required to consult with the Minnesota Administrative Uniformity Committee (AUC), on rules for the data content and format of standard, electronic health care administrative transactions.

The AUC is a broad-based, voluntary organization representing Minnesota's public and private health care payers, hospitals, health care providers and state agencies. It has served since 1992 to develop agreement among payers and providers on standardized administrative processes. The AUC acts as a consulting body to various public and private entities, but does not formally report to any organization and is not a statutory committee. It meets as a large committee of the whole, as well as through numerous

work groups and Technical Advisory Groups (TAGs). The work groups and TAGs reflect particular areas of expertise and divisions of labor with respect to different types of health care administrative transactions and processes. More information about the AUC is available at: www.health.state.mn.us/auc.

6) How can I find out about the activities and scheduled meetings of the Administrative Uniformity Committee (AUC)?

Answer: Information regarding the AUC and its activities can be found at the AUC website: www.health.state.mn.us/auc. In particular, a calendar on the website includes a posting of upcoming AUC meetings and activities, as well as links to meeting agendas, minutes, and other materials. AUC meetings and activities are open to the public.

7) When and how are the Minnesota Uniform Companion Guides/Rules updated?

Answer: The Minnesota Department of Health (MDH) is responsible for maintenance and updates of the Guides. At this time we plan for routine updates and maintenance of the Guides on an annual basis as described below.

Requests for changes to the Guides may be made by anyone at any time by submitting a form that can be found at www.health.state.mn.us/asa. Requests for changes will be reviewed and compiled for regular annual updates. In addition, MDH will respond to other possible needs for updating the Guides, arising for example from future changes to national standards or HIPAA regulations, or changes in state or federal law. The Guides will be updated in consultation with the Minnesota Administrative Uniformity Committee (AUC). Proposed updates or changes will be published in the State Register, followed by a public comment period, review of public comments, and publication of an announcement of the adopted changes.

III. COMPLIANCE AND ENFORCEMENT BY THE MINNESOTA DEPARTMENT OF HEALTH (MDH) (BEFORE REVIEWING THESE FAQs, PLEASE SEE ALSO CATEGORY I ABOVE)

1) What does the law say about compliance and enforcement? How will the law be enforced?

Answer: The Minnesota Department of Health (MDH) ensures compliance with MN Statutes § 62J.536 and related rules. The statute provides that:

- MDH is to achieve voluntary compliance to the extent practicable, and may provide technical assistance;
- Enforcement will be complaint-driven;
- MDH may investigate complaints, and is to seek informal resolution of complaints, for example through demonstrated compliance or a completed corrective action plan or other agreement;
- If informal resolution is not possible, MDH may impose civil money penalties of up to \$100 for each violation, but not to exceed \$25,000 for identical violations during a calendar year;

- Mitigating factors, such as whether attempts are being made to come into compliance, may be considered in determining any penalties; and,
- If a fine is levied, it may be appealed or a contested case hearing requested.

Even with the best communication and planning, providers and payers may still encounter possible problems during the initial implementation of standard, electronic administrative transactions.

We are committed to working with the industry to help identify and solve problems as quickly as possible while also achieving the goals of more standard, efficient transactions. As part of this commitment, **MDH will use its considerable regulatory flexibility to help minimize the possibility of delays or interruptions in routine business transactions during implementation of the rules.**

We understand that it is impractical to assume that all current paper transactions will be eliminated immediately on the dates the rules become effective. MDH's enforcement goal is not to collect fines for noncompliance, but to help assure that routine health care business transactions can flow more rapidly and efficiently. In enforcing the statute and related rules, **we will be especially interested in:**

- **whether good faith efforts are being made to comply;**
- **the extent of compliance efforts; and,**
- **progress toward compliance.**

In summary, **our approach to enforcement** and meeting the goals for standard, electronic transactions **will be flexible, practical, and consistent with an overall statutory enforcement policy of:**

- **seeking voluntary compliance and offering technical assistance;**
- **responding to complaints;**
- **working toward informal resolution of complaints; and,**
- **considering possible mitigating factors.**

2) As a group purchaser (payer), am I required to reject noncompliant claims?

Answer: Payers (or anyone acting on the payer's behalf) must be able to demonstrate they have the capability to accept Minnesota-compliant, standard, electronic transactions. However, during the initial implementation of standard, electronic transactions, MDH will not require payers to reject noncompliant claims. We encourage payers to work with providers to aid them in coming into compliance before taking steps to reject noncompliant claims.

3) Does my organization have to send the Minnesota Department of Health (MDH) information regarding its readiness for compliance?

Answer: MDH does not require any particular information at this time from either payers or providers regarding their readiness to comply with Minnesota Statutes, section 62J.536. In an effort to facilitate standard, electronic transactions, MDH has recently conducted voluntary surveys of payers to obtain information regarding points of contact for questions about establishing electronic connections, names of clearinghouses and

vendors, and other information to post on its website. The usefulness of these surveys and the need for possible additional required submissions of readiness status and other information to aid implementation of the rules is being evaluated.

4) If my trading partners are not in compliance with the law by the implementation dates, what should I do? When should I file a complaint? How do I file a complaint? What happens when a complaint is filed?

Answer: It will be important for trading partners to be communicating and working together before, during, and after the law's effective dates to be compliant. Per statute, enforcement of Minnesota's requirements for standard, electronic health care business transactions is complaint-driven. The statute also states that MDH is to seek informal resolution of complaints, and, if informal resolution is not possible, it may consider a number of mitigating factors before imposing any fines or penalties. During the initial implementation phases of the rules especially, we encourage trading partners to find ways to work together for compliance.

Parties may also consider filing a complaint of noncompliance with MDH for investigation and possible follow-up by the Department. However, it is important to note that the complaint filing and follow-up process is prescribed in statute, and that it requires specific steps in filing the complaint, providing notice to the subject(s) of the complaint, investigation of the complaint, and other steps. While complaints are an important and necessary option in some instances, the complaint process does require time and/or effort that may also be usefully spent in communicating about problems and working toward solutions.

Additional information about MDH's complaint-based enforcement is provided at www.health.state.mn.us/asa.

IV. FEDERAL HIPAA REGULATIONS (HIPAA TRANSACTIONS AND CODE SETS RULES; HIPAA PRIVACY AND SECURITY RULES)

1) What is HIPAA? Why do I have to know about HIPAA?

Answer: HIPAA stands for the Health Insurance Portability and Accountability Act. Title II of the Act includes a series of health care Administrative Simplification provisions that call for the establishment of standards for electronic health care transactions, unique identifiers for employers, health plans and health care providers, and privacy and security standards to protect health information.

Entities subject to HIPAA (known as 'covered entities') include 1) all health plans; 2) all health care clearinghouses; and 3) health care providers that choose to conduct administrative transactions electronically.

National standards for these areas are established by the Secretary of Health and Human Services through rulemaking process. Final HIPAA rules have been issued adopting standards and requirements for electronic transactions and code sets, a unique employer identifier, the national provider identifier, and privacy and security of health information. Compliance with the standards promulgated under HIPAA started April 14,

2003 with the HIPAA Privacy Rule. Civil and monetary penalties and federal criminal penalties may be imposed for the violation of HIPAA standards.

HIPAA calls for changes designed to streamline the administration of health care, eliminate proprietary formats and methods to codify and exchange information, and automate administrative processes to improve efficiencies in the health care industry and ultimately the quality of health care services provided.

Additional information about HIPAA can be found at <http://www.cms.hhs.gov/HIPAAGenInfo/>

2) What are HIPAA transactions and code sets rules? How do they relate to Minnesota's law and rules?

Answer: One group of federal regulations issued by the Secretary of Health and Human Services in response to the Administrative Simplification provisions of HIPAA was the HIPAA Transactions and Code Set Rules. Transactions are a set of defined activities involving the exchange of health care information (for example, a health care claim). Code sets are standard codified representations of certain health information that is included in a transaction (for example, the diagnosis of a patient using the International Classification of Diseases - ICD-9 code set).

The HIPAA Transactions and Code Sets Rules establish national standards to be used in the electronic exchange of selected transactions including transaction standards for health care claims or equivalent encounter information, claim payment/remittance advice, claim status inquiry and response, eligibility inquiry and response, coordination of benefits, referral certification and authorization inquiry and response, claim status inquiries and response, enrollment/disenrollment in a health plan, and health plan premium payment.

Standard code sets include 1) Healthcare Common Procedure Coding System (HCPCS) and the Current Procedure Terminology version 4 (CPT-4) for physician services and other health services; 2) HCPCS for medical supplies, orthotics and durable medical equipment; 3) ICD-9-CM Volumes 1 & 2 for coding all ambulatory and inpatient diagnosis; 4) ICD-9-CM Volume 3 for coding inpatient hospital procedures; 5) Code n Dental Procedures and Nomenclature (CDT) for dental services; 6) National Drug Codes (NDC) for coding drugs and biologics in retail pharmacy transactions.

National compliance with the HIPAA Transactions and Code Sets Rules started October 16, 2003 for all covered entities.

Relationship to Minnesota's Law and Rules: In 2007, Minnesota enacted a new law (Minnesota Statutes, Section 62J.536) requiring that all health care providers and group purchasers (health plans) exchange certain health care administrative transactions electronically. These transactions include health care claims, claim payment/remittance advice and eligibility. Consistent with HIPAA, health care providers and group purchasers are required to use the national standards and implementation guides adopted by the Secretary. In addition, to avoid inconsistent use of the implementation guides, providers and group purchasers are required to use a standard uniform 'companion guide', developed by the Commissioner of Health in consultation with the Minnesota Administrative Uniformity Committee (AUC).

More information about the HIPAA Transactions and Code Sets Rules can be found at http://www.cms.hhs.gov/TransactionCodeSetsStands/02_TransactionsandCodeSetsRegulations.asp#TopOfPage.

More information about the Minnesota Administrative Simplification requirements can be found at <http://www.health.state.mn.us/asa>.

3) I heard that HIPAA adopted new versions of the transactions and code sets rules? If there are new versions coming out, why is Minnesota implementing its rules now? How are providers, payers, and vendors supposed to implement Minnesota's rules now and also get ready for the new HIPAA rules?

Answer: Yes. After almost six year of implementation of the current HIPAA standards, new versions of the transactions have been recently adopted by the Secretary (January, 2009). These new versions affect all HIPAA electronic transactions and replaces the ICD-9-CM Volumes 1, 2 and 3 code set with the new ICD-10-CM (for diagnosis) and ICD-10-PCS (for inpatient hospital procedures). Implementation date for new version of the transactions is January 1, 2012. Compliance with the new ICD-10 code sets is October 1, 2013.

Minnesota is implementing its rules now because national compliance with the new versions of standards will not take place for two more years. Implementing the statewide uniform companion guides now will bring immediate efficiencies to the implementation of electronic transactions. Implementing these uniform companion guides now will also make it easier for providers, payers and vendors to transition to the new versions of the transactions, since several sections of the companion guides already take into account the requirements defined in the new versions of the standards.

4) What are HIPAA privacy and security rules?

Answer: The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes such as to protect public health. The HIPAA Privacy Rule creates, for the first time, national standards to protect individuals' medical records and other personal health information by giving patients more control over their health information, settings boundaries on when, how, by whom and for what purpose health records can be used and disclosed, and holding covered entities accountable with civil and criminal penalties, if they violate patients' privacy rights or other provisions of the Rule.

The HIPAA Privacy Rule was enacted to address the gaps that existed across the nation due to an uneven patchwork of federal and state privacy laws. Under this patchwork of laws, personal health information could be distributed -- without either notice or authorization -- for reasons that had nothing to do with a patient's medical treatment or health care reimbursement. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections will continue to apply over and above the new Federal privacy standards.

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Providing patients and enrollees with a Notice of Privacy Practices describing their privacy rights and how their information can be used and disclosed.
- Affording patients with the ability to access and receive a copy of their records, request restrictions on the uses and disclosures of their information, request amendments to their health information, and request an accounting of certain disclosures.
- Providing the minimum amount of health information needed to achieve the purpose of the disclosure (except when disclosure is for treatment purposes)
- Adopting and implementing internal written operating privacy policies and procedures.
- Training employees so that they understand and comply with the privacy policies and procedures.
- Designating an individual to be responsible for seeing that the privacy policies and procedures are adopted and followed.

All health and medical records and other personal health information held or disclosed by a covered entity in any form (paper, electronic, orally) is covered by the HIPAA Privacy Rule.

Compliance with the HIPAA Privacy Rule started April 14, 2003.

The recently enacted American Reinvestment and Recovery Act of 2009 (ARRA) makes important modifications and extensions to the current HIPAA Privacy Rule, including: applying the HIPAA Rule directly to business associates and other non-HIPAA covered entities;

- allowing patients to pay out of pocket for a health care service and request non-disclosure of the rendered service;
- authorizing increased civil monetary penalties for HIPAA violations;
- defining which actions constitute a breach (including some inadvertent disclosures) and requiring breach notification;
- requiring an accounting of all disclosures when using an electronic health record system; and,
- granting authority to state attorneys general to enforce HIPAA. Unless otherwise specified, the privacy provisions become effective on February 17, 2010.

More information about the HIPAA Privacy Rule can be obtained from <http://www.hhs.gov/ocr/privacy/index.html>.

The HIPAA Security Rule established a series of physical, technical and administrative safeguards that covered entities must implement to protect the confidentiality, availability and integrity of the electronic health information they maintain. Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information that the covered entity creates, receives, maintains, or transmits; protect

against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and ensure compliance by its workforce.

The HIPAA Security Rule established 42 different required standards and required or addressable implementation specifications that covered entities must comply with. All standards and those implementation specifications that are required must be implemented as prescribed by the Rule. When an implementation specification is addressable, the covered entity must assess whether it is reasonable and appropriate for the covered entity to implement it and, if not, document why not and implement an equivalent alternative safeguard measure.

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Adopting and implementing internal written operating security policies and procedures
- Training employees so that they understand and comply with the security policies and procedures.
- Designating an individual to be responsible for seeing that the security policies and procedures are adopted and followed
- Conduct a risk analysis
- Implement security procedures to ensure that all workforce have appropriate authorization and access to electronic PHI
- Implement a log-in and security audit and monitoring program
- Establish security procedures to guard against malicious software and address security incidents
- Implement security procedures to respond to damaged systems, perform periodic back-ups, establish a disaster recovery plan and emergency mode operations plan
- Conduct periodic technical and non-technical security evaluations
- Implement security procedures to limit physical access to areas where electronic PHI is housed and establish a facility security plan
- Control receipt/removal, handling and final disposal of electronic media containing e-PHI
- Implement security procedures to protect e-PHI from improper alteration or destruction and the integrity of e-PHI transmitted electronically

Compliance with the HIPAA Security Rule was required starting April 20, 2005.

More information about the HIPAA Security Rule can be obtained from <http://www.cms.hhs.gov/SecurityStandard/>.

5) Why do I have to know about HIPAA privacy and security rules – do they apply to me?

Answer: All health plans and health care clearinghouses are subject to comply with the HIPAA Privacy and Security Rules. Health care providers that conduct any of the HIPAA administrative transactions electronically are also subject to comply with the HIPAA Privacy and Security Rules. Covered entities are required to include on agreements with business associates the same privacy and security requirements they are subject to comply with.

Many providers are already subject to comply with the HIPAA Privacy and Security Rules since conducting transactions electronically is becoming the norm for doing business. Upon reaching the first implementation deadline in the Minnesota Statutes requiring health care providers to conduct certain transactions electronically (July 15, 2009), all health care providers meeting the standard, electronic exchange requirements of MN Statutes § 62J.536 will be subject to the HIPAA Privacy and Security Rules.

6) What do you have to do to comply with HIPAA privacy rule?

Answer: (*) *Note: the following information is provided to assist entities organize their work toward HIPAA compliance, and does not constitute legal advice. Organizations should consult with legal counsel prior to taking any actions prompted by the information provided herein.*

The most important first step that you can take is to read and understand the requirements under the HIPAA Privacy Rule.

With respect to the HIPAA Privacy Rule, the following ten steps will assist you organize your compliance tasks.

1. Organize your privacy compliance plan: Prepare a formal plan for achieving compliance, document current privacy practices and prescribed requirements from the HIPAA Privacy Rule, and develop a working timeline for compliance.

2. Appoint a Privacy Official: The privacy official is responsible for the development and implementation of the policies and procedures required by the HIPAA Privacy regulations. The privacy official may also serve as the person designated to receive complaints and provide further information about matters covered by the privacy notice.

3. Develop and plan the dissemination of a Notice of Privacy Practices: Including the standard notice introductory information, describing the individual privacy rights, how their information can be used and disclosed, your privacy official's contact information, a reference about how consumers can file a complaint, and a acknowledgment of receipt. Make the Notice available to consumers at the first (or next) delivery of service. Make a good faith effort to obtain the individual's acknowledgement of receipt.

4. Develop written policies and procedures regarding the uses and disclosures of personal health information: Adopt or develop required forms to implement your privacy policies and procedures. Policies and procedures related to the use and disclosure of protected health information should cover:

- Uses and Disclosures for Treatment, Payment and Health Care Operations
- Uses and Disclosures with the Individual's Opportunity to Agree or Object
- Uses and Disclosures that Require Individual Authorization
- Uses and Disclosures that Do Not Require Individual Consent, Authorization or the Opportunity to Agree or Object

5. Establish procedures for minimum necessary uses and disclosures: Only use or disclose the information that is needed to accomplish the intended purpose, when applicable.

6. Establish Procedures to document and account for disclosures: Certain disclosure of health information must be accounted for, such as disclosures to public health, for research purposes, and others, in case a consumer wants to request an accounting of disclosures of their health information.

7. Plan for the Implementation of Individual Privacy Rights: Under HIPAA, individuals have rights to:

- Receive a Notice of Privacy Practices
- Access and copy the health information
- Request an amendment of their health information
- Request an accounting of certain disclosures of their health information
- Request restrictions on the use and disclosure of their health information
- Request communication by alternative means and to alternative locations
- File complaints regarding the handling of their health information

8. Evaluate Your Business Associate Relationships: Evaluate all your business relationships and determine which require a Business Associate agreement. You will need a Business Associate agreement with one of your vendors if the answer to all three of the following questions is "Yes": 1) does your organization have a contractual relationship with the vendor to perform services or activities on behalf of your organization?; 2) does your organization need to supply the vendor with personal health information or access to personal health information in order for the vendor to perform its service or activity on your behalf? and 3) is the service or activity a service or activity other than treatment?

9. Implement appropriate use and disclosure restrictions in certain circumstances: Strict restrictions apply if the use and disclosure of protected health information relates to marketing activities, fundraising activities and psychotherapy notes.

10. Plan and Conduct Privacy Training of Workforce: Train your workforce about your privacy policies and procedures; establish and designate a contact person and a process to receive complaints.

Additional guidelines and resources to assist you with implementing the HIPAA Privacy Rule can be found at <http://www.hhs.gov/ocr/privacy/>

7) What do you have to do to comply with HIPAA security rule?

Answer: (*) *Note: the following information is provided to assist entities organize their work toward HIPAA compliance, and does not constitute legal advice. Organizations should consult with legal counsel prior to taking any actions prompted by the information provided herein.*

The most important first step that you can take is to read and understand the requirements under the HIPAA Security Rule.

With respect to the HIPAA Security Rule, the following ten steps will assist your organization in its work towards compliance.

1. Organize your security compliance plan: Prepare a formal plan for achieving compliance, document current security practices and prescribed requirements from the HIPAA Security Rule, and develop a working timeline for compliance. Security requirements are organized into four major categories: administrative, physical and technical safeguards and additional requirements.

2. Appoint a Security Official: The security official is responsible for the development and implementation of the policies and procedures required by the HIPAA Security regulations. The security official may also serve as the person designated to receive complaints and provide further information about matters covered by the privacy notice.

3. Evaluate addressable implementation specifications: Understand the difference between required and addressable implementation specifications. All standards and those implementation specifications that are required by the Security Rule must be implemented as prescribed. Addressable implementation specifications must be evaluated by organizations to determine if it would be reasonable and appropriate for the organization to implement them. If the organization determines it is not reasonable and appropriate, then it must document the reasons why not and plan to implement an equivalent alternative safeguard measure.

4. Evaluate, plan and implement administrative safeguards and develop corresponding written policies and procedures: Administrative safeguards include (an 'R' next to the safeguard means required; an 'A' next to the safeguard means addressable):

- Security management process to prevent, detect, contain and correct security violations (R), including:
 - Planning and conducting a security risk analysis (R)
 - Develop and implement a risk management measures to reduce risks and vulnerabilities (R)
 - Establish a sanction policy (R)

- Workforce security to ensure appropriate access (and prevent inappropriate access) to health information (R), including:
 - Authorization and/or supervision of workforce members (A)
- Security awareness and training of workforce (R), including:
 - Procedures for creating, changing and safeguarding passwords (A)
- Contingency plans to respond to emergencies that affect systems where health information is maintained (R), including:
 - Developing and implementing a data back-up plan (R)
- Business associate contracts and other arrangements (R), including:
 - Include in written contract or other arrangements assurances that health information will be appropriately safeguarded (R)

5. Evaluate, plan and implement physical safeguards and develop corresponding written policies and procedures: Physical safeguards include (an 'R' next to the safeguard means required; an 'A' next to the safeguard means addressable):

- Implement facility access controls (R), including:
 - Developing a facility security plan to safeguard the facility and equipment from unauthorized access (A)
 - Maintenance records documenting repairs and modifications to physical components (A)
- Policies and procedures related to workstation use, specifying the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of workstations that can access personal health information (R)
- Device and media control policies governing the receipt and removal of hardware and electronic media that contain personal health information (R), including:
 - Disposal (final disposition) policies and procedures (R)
 - Data backup and storage before movement of equipment (A)

6. Evaluate, plan and implement technical safeguards and develop corresponding written policies and procedures: Technical safeguards include (an 'R' next to the safeguard means required; an 'A' next to the safeguard means addressable):

- Technical policies and procedures to ensure access controls (R), including:
 - Assigning a unique name and/or number for identifying and tracking user identity (R)
 - Automatic logoff policies (A)

- Procedures to verify and authenticate a person or entity seeking access to personal health information (R)
- Technical security measures to guard against unauthorized access to personal health information being transmitted electronically (R), including:
 - Mechanisms to encrypt electronic personal health information (A)

7. Evaluate, plan and implement additional security requirements: Additional security requirements include:

- General requirements such as ensuring confidentiality, integrity and availability of electronic personal health information; ensuring compliance with all standards; ensuring compliance with all required implementation specifications; ensuring assessment of addressable implementation specifications; and ensuring periodic review and modification, as appropriate, of all security measures, policies and procedures.
- Business associate contract requirements, including requiring contractors to meet (and provide assurances) appropriate administrative, physical and technical safeguards and provide assurance to that effect; requiring that subcontractors of business associates to also meet appropriate safeguards; and requiring report of security incidents.
- Documentation requirements, including written policies and procedures (maintained for at least 6 years) to comply with standards, implementation specifications and other requirements; documents are made available to persons responsible for implementing requirements; and documentation is reviewed and updated periodically.

8. Plan and Conduct Security Training of Workforce: Train your workforce about your security policies and procedures; establish and designate a contact person and a process to receive complaints.

Additional guidelines and resources to assist you with implementing the HIPAA Privacy Rule can be found at <http://www.cms.hhs.gov/SecurityStandard/>.

8) Where can I find the HIPAA Implementation Guides? Does my organization need to buy them in order to be compliant?

Answer: The HIPAA Implementation Guides, the documents used to implement the national electronic standards adopted by HIPAA for the named administrative transactions, can be found at the following locations:

- For retail pharmacy transactions, they are available from the National Council for Prescription Drug Programs (NCPDP) at <http://www.ncdp.org>.
- For all other transactions, they are available from the Washington Publishing Company at <http://www.wpc-edi.com>. These implementation guides are developed by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 Committee (<http://www.x12.org>).

If you have general questions about the implementation guides, you can begin with your practice management software vendor, health care clearinghouse, or the EDI contact at your trading partner organizations.

X12 Committee responses for formal interpretations of their implementation guides are available at <http://www.x12.org/rfis/index.cfm>.

The X12 implementation guides for the version of the transactions currently required to be implemented by the HIPAA Transactions and Code Sets Rules (version 004010 plus A1 addenda) are available for a fee from the Washington Publishing Company (<http://www.wpc-edi.com/hipaa>.)

There is a fee for non-members of NCPDP to obtain a copy of the NCPDP implementation guides for the retail pharmacy transactions.

In most cases, depending on the size of the organization and the volume of transactions being done, the organization will depend on and work with their practice management software vendor or health care clearinghouse to meet the HIPAA Transactions and Code Sets requirements and may not need to purchase the implementation guides.

9) Where can I find the NCPDP (National Council of Prescription Drug Programs) guides? Does my organization need to buy them in order to be compliant?

Answer: The NCPDP implementation guides or standard manuals used in retail pharmacy transactions provide technical guidance and education on how to implement the standard format for these transactions. The guides are available from the National Council for Prescription Drug Programs (NCPDP) at <http://www.ncdp.org>. There is a fee for non-members of NCPDP to obtain a copy of the NCPDP implementation guides.

In most cases, depending on the size of the organization and the volume of transactions being done, the organization will work with (and depend on) their practice management software vendor or health care clearinghouse to meet the HIPAA Transactions and Code Sets requirements and may not need to purchase the implementation guides.

V. IMPLEMENTATION, BECOMING COMPLIANT WITH THE LAW AND RULES

1) What are the options for providers to connect electronically with payers?

Answer: There are many options for providers to connect electronically with payers, ranging from direct Electronic Data Interchange (EDI) connections, to contracting with a variety of vendors and services (“clearinghouses”, “billing services”, etc.), to secure, web-based “direct data entry” tools that allow providers to directly key in and transmit Minnesota compliant claims to payers. It will be important to evaluate options to find those that best meets your business needs. Many providers are consulting with their associates, payers, business advisors, professional and trade associations, and others for advice and possible recommendations.

2) Does the MN Dept of Health (MDH) or anyone have a list of recommended vendors?

Answer: MDH does not have a list of recommended vendors. As noted in the answer to question 1) above, there are many options for providers to connect with payers electronically, and it is important for providers to find the option that best meets their needs. MDH does not require use of any particular vendor or services and does not endorse or recommend any particular vendors.

3) Will MDH be providing a low cost or free way to connect and send the required electronic transactions?

Answer: The Minnesota Department of Health (MDH) does not have responsibilities or resources for offering free or low cost electronic connectivity and MDH will not be providing such a service.

Please note: Another state agency, the Minnesota Department of Human Services (DHS), maintains a secure web portal for providers to submit claims for free for patients who are covered under DHS public programs such as Medical Assistance or MinnesotaCare (for further information, see: <https://mn-its.dhs.state.mn.us/login.html>).

In addition, MDH is consulting with the Minnesota Administrative Uniformity Committee (AUC) on rules for standard, electronic health care administrative transactions. An AUC member, the Minnesota Council of Health Plans, recently announced the availability of a direct data entry web portal for providers to submit health care claims to participating Minnesota health plans at no cost to the provider. (For additional information about this option, please see: <http://www.mnhealthplans.org/tools/links.cfm> regarding [Provider tool for submitting claims.](#)) We are not aware whether there may be other web portal options available at low cost or no cost to providers. Again, as noted previously in these FAQs, MDH does not require or endorse any products or vendors.

4) Where can I find names and contact information for group purchasers (payers) and health care providers that are covered by the law? How are covered group purchasers/payers and health care providers identified in Minnesota?

Answer: We have posted a preliminary, informational list of insurance carriers and Third Party Administrators (TPAs) licensed in Minnesota that are covered by MN Statutes § 62J.536 at: www.health.state.mn.us/asa. This list is intended only as an informational resource. It is maintained to be as accurate as possible given information available but is subject to change. It is NOT a legal determination by the State of Minnesota or any other organization of all possible payers covered by Minnesota Statutes, section 62J.536.

We do not have a comparable list of providers in Minnesota covered by MN Statutes § 62J.536. Please see FAQs in section I above with additional information regarding providers covered by the statute.

5) What information do I need (what questions do I need to ask) to connect electronically? Where can I find information on how to connect?

Answer: Providers should contact their payers, or check payers' websites, for information on how to connect electronically.

Please also note: MDH will be posting the results of recent short surveys of payers that provided information to facilitate connecting electronically. However, as with most surveys,

not all payers responded, and not all responses are equally detailed or accurate. As a result, at this time we still recommend that providers contact payers (or access information often available on payers' websites) for information needed to connect electronically.

VI. QUESTIONS SPECIFIC TO EACH OF THE COVERED TRANSACTIONS (ELIGIBILITY INQUIRY AND RESPONSE; CLAIMS; PAYMENT AND REMITTANCE ADVICE)

A. ELIGIBILITY INQUIRY AND RESPONSE

1) We know that as of January 15, 2009, when we check a patient's eligibility for insurance coverage and benefits, it has to be done electronically. What does "electronically" mean for us? Can eligibility and benefits ever be verified by calling and talking to a live person, or by calling and using an automated Interactive Voice Response (IVR) telephone system?

Answer: "Electronically" means that initial eligibility inquiries and responses must be exchanged either via compliant internet ("web") or "electronic data interchange" (EDI) connections. Interactive Voice Response (IVR) is not compliant for this initial exchange. If, after an initial compliant exchange (via web or EDI) additional information or review is needed, other options that may be available from payers may be used, including IVR. Many in the industry are transitioning away from the IVR systems they had made available to check eligibility and are putting into place compliant web-based and EDI alternatives. We appreciate and encourage everyone's good faith efforts in making this transition.

B. CLAIMS

1) Each of the MN AUC companion guides include Required, Situational or Not Considered for Processing in the Usage column. Do the required fields/elements have to be used in processing?

Answer: ALL of the segments/fields/elements that are classified as REQUIRED in the HIPAA Implementation Guides (i.e., 837P 00401A1, NCPDP 5.1) must be sent by the submitter. In some instances that are identified in the MN Uniform Companion Guides, the receiver may choose to not use the submitted element in the processing of the transaction.

2) We often deny bills for multiple reasons. What is the MN requirement for denied bills? (i.e. Is an 835 required?)

Answer: Claims transactions that have passed basic edits and that have not been rejected due to general envelope, formatting or transaction validation issues, and for which claim processing has been initiated in the payer's system, require a Health Care Claim Payment and Remittance Advice (835). The 835 transaction must document the claim adjustments via Claim Adjustment Reason Codes (CARCs) + Remittance Advice Remark Codes (RARCs), including claim denials.

3) Can we reject the transaction if the claim number is not entered?

Answer: There are several claim numbers in the transaction. All are situational.

- The Original Reference Number (ICN/DCN) is situational, and only required when claim submission reason codes are 6 (Corrected claim), 7 (Replacement claim) or 8 (Void) and the payer has assigned a number to the original claim.
- The Property and Casualty Claim Number is situational and should be reported when known. You should not deny the bill simply because it is missing this number but you could deny it if you are unable to match the bill to a P&C claim. (The claim number field is situational but is required if the claim is a Property and Casualty or Worker's Compensation claim. As such, if a clearinghouse knows that the destination group purchaser is a Property and Casualty-only carrier, they can edit it at the clearinghouse and deny it back to the provider to obtain the Property and Casualty claim number.)
- The Repriced Claim Number is situational.

4) Is TIN (Tax Identification Number) Required in each of the eBill types?

a) 837 I,P,D?

b) NCPDP, NCPDP reversal

Answer: Yes. The TIN is required for the billing provider and can only be reported in specific segments. The NPI must be provided in the primary identifier segments. The TIN must be reported in the BILLING PROVIDER Secondary Identification Information segment (837s) and the PAYEE Additional Identification segment (835). The Tax ID of a pharmacy is not required on the NCPDP claim. The NPI of the Pharmacy is required, as is the NPI (and in some cases the DEA#) of the Prescriber.

5) How do we Determine state of jurisdiction?

- a. Can we base on TIN?
- b. Do we begin with Service Facility and work back through other state attributes? For example:
 - i. First look for Service Facility state and if blank use:
 - ii. Provider Pay-to State, if blank use:
 - iii. Provider Billing State.

Answer: Payers should determine state of jurisdiction the same way they do now based on state laws, federal laws, where the accident occurred, where insurance resides for each party, etc. The Minnesota Uniform Companion Guides do not dictate how state of jurisdiction is determined but rather provide a way to report state of jurisdiction once it has been determined.

For example, if the question of jurisdiction relates where to the services are being rendered, then the service facility location or rendering provider location would be used. If the question is related to the billing of services, then the billing provider location should be used.

6) How do I send claims attachments in order to be compliant with the law?

Answer: Claims attachments are addressed in the front matter of all three Minnesota Uniform Companion Claims Guides (Professional, Institutional, and Dental), in section 4.2.3.4.

Supplemental Best Practices for the submission of claims attachments can be found on the Minnesota Administrative Uniformity Committee (AUC) website at:

- <http://www.health.state.mn.us/auc/profguide.htm> (for professional services);
- <http://www.health.state.mn.us/auc/instguide.htm> (for institutional services);
- <http://www.health.state.mn.us/auc/dentguide.htm> (for dental services).

7) Does the Minnesota Uniform Companion Guide address how to bill for MinnesotaCare (MNCare) Tax on a claim?

Answer: The Minnesota Uniform Companion Claims Guides offer guidance on this topic in Appendix E of the Professional and Institutional Minnesota Uniform Claim Companion Guides, and in Appendix D of the Minnesota Uniform Dental Claim Guide. For copies of the Guides, go to:

<http://www.health.state.mn.us/asa/rules.html>.

C. PAYMENT REMITTANCE ADVICE

1) When the Remittance Advice component of the law goes into effect on December 15, 2009, does it also require that payments be sent electronically? Does my organization need to be ready to send “electronic funds transfer” (EFT) payments to health care providers as well?

Please also note: The Minnesota Department of Health (MDH) encourages electronic payment (electronic funds transfer, EFT) as a further means of reducing health care administrative costs and burdens. However, MN Statutes § 62J.536 does not require electronic payment (EFT). Group purchasers and providers may be subject to other requirements or trading partner agreements which require the transmission of an electronic payment. It is recommended that each organization familiarize itself with its payment procedures as it may relate to the remittance advice implementation date.

VII. OTHER/MISC.